

## Passaggi per l'hacking su Metasploitable con vsftpd

1. **Avviare Metasploit** Avvia Metasploit tramite il comando `msfconsole` nel terminale.
2. **Scansione della macchina Metasploitable** Esegui una scansione dei servizi attivi sulla macchina Metasploitable utilizzando `nmap` con l'opzione `-sV` per ottenere informazioni sui servizi e sulle versioni.

```
nmap -sV 192.168.1.149
```

Questo ci permette di identificare i servizi attivi e le versioni, inclusa la configurazione di `vsftpd` sulla porta 21.

3. **Ricerca dell'exploit per vsftpd** All'interno di Metasploit, esegui una ricerca per un exploit specifico per `vsftpd` utilizzando il comando `search`:

```
sql
search vsftpd
```

Trova un exploit adatto e utilizzalo con il comando `use` seguito dal path dell'exploit.

4. **Configurazione delle opzioni dell'exploit** Una volta selezionato l'exploit, utilizza il comando `show options` per visualizzare i parametri necessari da configurare. Assicurati di impostare correttamente l'indirizzo IP della macchina Metasploitable come `RHOSTS`:

```
arduino
set RHOSTS 192.168.1.149
```

Verifica nuovamente le opzioni configurate utilizzando `show options` per assicurarti che tutti i parametri siano corretti.

5. **Scelta e configurazione del payload** Verifica i payload disponibili per l'exploit con il comando `show payloads`. Scegli il payload appropriato e verifica nuovamente i parametri necessari utilizzando `show options`.
6. **Esecuzione dell'exploit** Una volta configurato tutto correttamente, sei pronto per lanciare l'attacco con il comando `exploit`.
7. **Verifica dell'accesso e creazione della cartella** Se l'attacco ha successo, otterrai una shell sulla macchina Metasploitable. Verifica la connessione utilizzando comandi come `ifconfig` per confermare l'indirizzo IP della macchina Metasploitable. Successivamente, crea la cartella `test_metasploit` nella directory radice (`/`) con il comando:

```
bash
mkdir /test_metasploit
```

8. **Conclusione** Se hai seguito correttamente i passaggi e hai ottenuto l'accesso alla shell sulla macchina Metasploitable, avrai creato con successo la cartella `test_metasploit` come richiesto.